NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 2810.1A
Effective Date: May 16, 2006
Expiration Date: May 16, 2011

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: Security of Information Technology

Responsible Office: Office of the Chief Information Officer

SECTION I NASA IT SECURITY PROGRAM

Chapter 1 Introduction, Laws and Regulations, Capital Planning, and Metrics

1.1 Introduction

1.1.1 The overall objective of the Information Technology (IT) Security Program is to provide requirements and direction to ensure that safeguards for IT resources (i.e., data, information, applications, and systems) are integrated into and support NASA's missions and functional lines of business.

1.1.2 Security categorization standards for information and information systems provide a common framework and understanding for expressing security that, for the Federal Government, promotes: (i) effective management and oversight of information security programs, including the coordination of information security efforts throughout the civilian, national security, emergency preparedness, homeland security, and law enforcement communities; and (ii) consistent reporting to the Office of Management and Budget (OMB) and Congress on the adequacy and effectiveness of information security policies, procedures, and practices.

1.1.3 The FIPS 199 establishes security categories for both information and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.

1.1.4 The security categories of information and IT resources that require protection are as follows:

a. Confidentiality. Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

b. Integrity. Guarding against unauthorized information modification or destruction, which includes ensuring information non-repudiation and authenticity. Loss of integrity is the unauthorized modification or destruction of information.

c. Availability. Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

1.2 Laws and Regulations

1.2.1 The E-Government Act of 2002, Pub. L. 107-347, recognizes the importance of IT security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the "Federal Information Security Management Act" (FISMA), requires each Federal agency to develop, document, and implement an agencywide IT security program to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, support service contractor, or source. FISMA directs the National Institute of Standards and Technology (NIST) to publish the appropriate standards and guidance necessary for agencies to implement FISMA.

1.2.2 FISMA, along with the Paperwork Reduction Act of 1995 and the Information Technology Management Reform Act of 1996 (Clinger-Cohen Act), explicitly emphasizes that a risk-managed policy for cost-effective IT security and information security principles and practices must be addressed throughout the life cycles of the agency's information systems.

1.2.3 NASA's security protections shall be commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of the information or information system.

1.2.4 FISMA holds agency heads responsible for ensuring that IT security management processes are integrated with agency strategic and operational planning processes. NASA shall integrate IT security into its capital planning and investment process, its contracting and acquisition strategies, and its program and project life cycle.

1.3 Policy Requirements

1.3.1 NASA IT security polices, requirements, and procedures shall be:

a. Established to implement NIST publications on IT security to support the missions of NASA.

b. Based on the analysis of security risks and the cost-effective reduction of risks to an acceptable level.

c. Apply throughout the life cycle of the information and the information system, and the life cycle processes of programs and projects.

d. Measured and reviewed at least annually to validate effectiveness and to ensure compliance with current Federal policies and guidance.

1.3.2 NASA shall respond to new threats and vulnerabilities, which require policies, procedures, and security controls to be reviewed and modified, on a continuing basis to ensure that information and information systems are adequately protected. To accommodate new threats and vulnerabilities in policy and procedures, NASA shall:

a. Issue NASA Information Technology Requirements (NITRs) documents to keep the NASA IT Security Program current with changes in the IT environment and with changes in Federal policy and guidelines. NASA NITRs shall be incorporated into future revisions of this NPR. Once a NITR has been incorporated into the next revision of the NPR 2810.1, the NITR shall be canceled.

b. Utilize Standard Operating Procedures (SOPs) to ensure consistent implementation and develop educational, technical guidance, and awareness and training materials to ensure a competent, skilled, and up-to-date workforce. Request for deviating from SOPs shall be addressed to the OCIO for approval or disapproval.

c. The OCIO will publish Directive Letters as required to convey short-term requirements such as metrics deliverables.

d. Revisions to NASA security policies, requirements, and procedures (e.g., NITRs and Directive Letters) that affect NASA procurement and non-procurement instruments shall be implemented through action by the contracting officer.

1.4 Capital Planning

1.4.1 Capital Planning Overview

1.4.1.1 FISMA charges agencies with integrating IT security into the Capital Planning and Investment Control (CPIC) processes, which have previously been performed independently by security and capital planning practitioners. NASA must effectively bridge the gap between IT security and capital planning to ensure that available funding is applied toward protecting NASA's IT investments. OMB requires that annual budget packages, submitted under OMB Circular A-11, Exhibits 53 and 300, specifically include the IT security component.

1.4.1.2 FISMA, OMB Circular A-130, Appendix III, and General Accountability Office's (GAO) Federal Information System Controls Audit Manual (FISCAM) security requirements all relate to NIST Special Publication (SP) 800-26, Security Self-Assessment Guide for Information Technology Systems, and the NIST SP 800-53, Recommended Security Controls for Federal Information Systems, because minimum baseline security requirements are discussed.

1.4.1.3 The capital planning requirements contained in FISMA and OMB Circular A-11 impact the capital planning process at Federal agencies. OMB Circular A-11 directs agencies to complete Exhibit 300s and an Exhibit 53.

1.4.1.4 The FISMA report directly impacts the capital planning process. OMB requires that all agencies are in compliance with NIST SP. It is mandatory that the FIPS are followed. As part of this requirement, NASA shall capture all known weaknesses in the Plan of Action and Milestones (POA&M) process. The POA&M is a document that lists the steps necessary to remediate known weaknesses. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. (See Appendix B, Glossary for a definition of the POA&M.) The weaknesses identified are logged into the POA&M. NASA must then determine the costs and timeframes associated with mitigating the vulnerability and correcting security deficiencies. As appropriate, these costs are captured in the Exhibit 300 and rolled into the Exhibit 53, which provides an overview of NASA's IT portfolio. (See Appendix B, Glossary for a high-level definition of Exhibits 300 and 53.) The Exhibit 53 includes a roll up of all Exhibit 300s and additional IT expenses from across NASA. All IT investments are identified by mission area. Investment information includes the budget year and life cycle cost, as well as the percentage of the costs that are devoted to IT security. All costs listed in the Exhibit 300s are totaled across NASA to provide an overall picture of the NASA's IT portfolio.

1.4.2 Capital Planning Requirements

1.4.2.1 NASA shall follow NIST SP 800-65, Integrating Security into the Capital Planning and Investment Control Program, for guidance on capital planning.

1.4.2.2 NASA capital planning and investment strategies, at all levels, shall, as a minimum:

a. Identify the IT security requirements necessary for certification and accreditation (C&A) of all IT investments and ensure that resources are available.

b. Provide the resources necessary to implement and operate IT security requirements throughout the life cycle of the IT investment.

c. Track IT security requirements, as a critical element, in the CPIC process and all program management reviews.

d. Require the identification and approval of funding necessary to remediate weaknesses identified in NASA system's POA&M as dictated by the most recent OMB requirements.

e. Require that IT security funding is integrated into NASA's Exhibit 300s and Exhibit 53s and that the exhibits are cross-referenced to NASA's Reporting Repository and Development Database (R2D2).

1.4.2.3 All NASA program reviews, including Independent Assessments (IA), Non-Advocate Reviews (NAR), and the program and project plans shall include the following critical elements:

a. Identify the information category, potential impact, and the Federal Laws restricting distribution of the information that is expected to be processed, stored, or handled throughout the life cycle of the program or project.

b. Identify the IT security requirements necessary for certification and accreditation of all IT investments.

c. Identify the resources necessary to implement IT security requirements throughout the life cycle of the IT investment.

d. Track IT security requirements until mitigated as a critical risk element.

1.4.2.4 NASA Space Act Agreements shall address capital planning, if appropriate, to include:

a. Identifying the information category and potential impacts.

b. Identifying the Federal Laws restricting distribution of the information that will be processed, stored, or handled.

c. Specifically assigning IT security roles and responsibilities to the Space Act Agreement parties.

d. Identifying and documenting the approval authority necessary to grant exceptions to Federal Laws and NASA policies and requirements.

e. Providing for the reporting and investigation of IT security incidents and non-compliance with Federal Laws and NASA policies.

f. Identifying the IT security requirements necessary for C&A of all IT investments.

g. Providing the necessary resources for implementing IT security requirements throughout the life cycle of an IT investment.

1.5 Metrics

1.5.1 The obligation to measure performance and reduce cost is driven by Federal regulatory and NASA requirements. These measurements shall be based upon NASA's goals and objectives, be designed to provide substantive justification for decision-making, and be utilized to measure the effectiveness of the IT Security Program, policies, and requirements. IT Security Program measurement goals and objectives are not static and will be adjusted as the operating environment, threats, and requirements evolve.

1.5.2 Metrics Requirements

1.5.2.1 NASA IT security metrics will be presented to Center Directors and Associate Administrators and will be used to assess the performance of Centers and Agency installations.

1.5.2.2 NASA IT security metrics shall be established by the OCIO Directive Letters.

1.5.2.3 NASA IT security metrics shall address specific IT security controls, assessment findings, or audit findings.

1.5.2.4 NASA IT security metrics shall be analyzed and evaluated by the OCIO, at least annually, for effectiveness in risk reduction and for cost versus impact on return on investment.

1.5.3 Additional IT Security Program References.

a. NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems.

b. NIST SP 800-53, Recommended Security Controls for Federal Information Systems.

c. NIST SP 800-55, Security Metrics Guide for IT Systems.

d. NIST SP 800-64, Security Considerations in the Information System Development Life Cycle.

e. NIST SP 800-65, Integrating Security into the Capital Planning and Investment Control Program.

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | Chapter11 | Chapter12 | Chapter13 | Chapter14 | Chapter15 | Chapter16 | Chapter17 | Chapter18 | Chapter19 | Chapter20 | Chapter21 | AppendixA | AppendixB | ALL |

| NODIS Library | Legal Policies(2000s) | Search |

DISTRIBUTION:
NODIS